Clark County Land Reutilization Corporation

Cyber Security and Information Assurance Policy

Adopted 10/31/2018

Policy Brief & Purpose

The Clark County Land Reutilization Corporations' cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our organization's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Policy Elements

Confidential Data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Unpublished future development plans
- Personal information

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Protect Personal and Organization-Owned Devices

When employees use their digital devices to access organization emails or accounts, they introduce security risk to our data. We advise our employees to keep their personal and organization issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Ensure they do not leave their devices exposed or unattended.
- Log into organization accounts and systems through secure and private networks only.
- Notify IS Department of suspicious activity.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive organization-issued equipment they will receive instructions for Password management. They should follow instructions to protect their devices and refer to our IS Department they have any questions.

Keeping Emails Safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of click-bait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If an employee isn't sure that an email they received is safe, they can refer to our IS Department.

Manage Passwords Properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advice our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.

- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

Transfer Data Securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our IS Department for assistance.
- Share confidential data over the organization's network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

The IS Department needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT Specialists must investigate promptly, resolve the issue and send an organization-wide alert when necessary.

Our managers are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional Measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to HR/ IS Department.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in organization systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

Take Security Seriously

Everyone, from our community members and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.